

CLAIMS

What is claimed is:

- 1 1. A method for recognizing virus signatures, comprising  
2 (a) identifying a list of virus signatures;  
3 (b) combining the list of virus signatures into a tree of virus signatures; and  
4 (c) comparing data against the tree of virus signatures for virus signature  
5 recognition.
- 1 2. The method as recited in claim 1, wherein the virus signatures each include a  
2 sequence of characters.
- 1 3. The method as recited in claim 2, wherein the tree includes a plurality of  
2 branches each including a sequence of characters.
- 1 4. The method as recited in claim 3, wherein a portion of the branches corresponds  
2 to a plurality of the virus signatures.
- 1 5. The method as recited in claim 4, wherein the efficiency of the virus signature  
2 recognition is improved.
- 1 6. The method as recited in claim 4, wherein the branches include further sub-  
2 branches each corresponding to at least one virus signature.
- 1 7. The method as recited in claim 4, wherein the characters include wildcards.

- 1 8. The method as recited in claim 4, wherein the characters of the tree of virus  
2 signatures are obfuscated to prevent detection by the comparison.
- 1 9. The method as recited in claim 1, wherein the branches include upper branch  
2 portions and lower branch portions.
- 1 10. The method as recited in claim 9, wherein the comparing includes comparing the  
2 data against the upper branch portions of the tree.
- 1 11. The method as recited in claim 10, wherein the comparing further includes  
2 comparing the data against the lower branch portions of the tree if the data was  
3 successfully compared to the upper branch portions associated with the lower  
4 branch portions.
- 1 12. The method as recited in claim 11, wherein a virus signature is determined to be  
2 recognized upon the successful comparison of the data against an entirety of at  
3 least one branch that includes all of the characters of one of the virus signatures.
- 1 13. The method as recited in claim 11, wherein data is eligible to be declared clean  
2 upon the unsuccessful comparison of the data against an entirety of at least one  
3 branch that includes all of the characters of one of the virus signatures.
- 1 14. A computer program product for recognizing virus signatures, comprising  
2 (a) computer code for identifying a list of virus signatures;  
3 (b) computer code for combining the list of virus signatures into a tree of virus  
4 signatures; and  
5 (c) computer code for comparing data against the tree of virus signatures for virus  
6 signature recognition.

- 1 15. The computer program product as recited in claim 14, wherein the virus  
2 signatures each include a sequence of characters.
- 1 16. The computer program product as recited in claim 15, wherein the tree includes  
2 a plurality of branches each including a sequence of characters.
- 1 17. The computer program product as recited in claim 16, wherein a portion of the  
2 branches corresponds to a plurality of the virus signatures.
- 1 18. The computer program product as recited in claim 17, wherein the efficiency of  
2 the virus signature recognition is improved.
- 1 19. The computer program product as recited in claim 17, wherein the branches  
2 include further sub-branches each corresponding to at least one virus signature.
- 1 20. The computer program product as recited in claim 17, wherein the characters  
2 include wildcards.
- 1 21. The computer program product as recited in claim 17, wherein the characters of  
2 the tree of virus signatures are obfuscated to prevent detection by the  
3 comparison.
- 1 22. The computer program product as recited in claim 14, wherein the branches  
2 include upper branch portions and lower branch portions.
- 1 23. The computer program product as recited in claim 22, wherein the comparing  
2 includes comparing the data against the upper branch portions of the tree.

1 24. The computer program product as recited in claim 23, wherein the comparing  
2 further includes comparing the data against the lower branch portions of the tree  
3 if the data was successfully compared to the upper branch portions associated  
4 with the lower branch portions.

1 25. The computer program product as recited in claim 24, wherein a virus signature  
2 is determined to be recognized upon the successful comparison of the data  
3 against an entirety of at least one branch that includes all of the characters of one  
4 of the virus signatures.

1 26. The computer program product as recited in claim 24, wherein data is eligible to  
2 be declared clean upon the unsuccessful comparison of the data against an  
3 entirety of at least one branch that includes all of the characters of one of the  
4 virus signatures.

1 27. A system for recognizing virus signatures, comprising  
2 (a) logic for identifying a list of virus signatures;  
3 (b) logic for combining the list of virus signatures into a tree of virus signatures; and  
4 (c) logic for comparing data against the tree of virus signatures for virus signature  
5 recognition.

1 28. A method for recognizing virus signatures with improved efficiency, comprising  
2 (a) identifying a list of virus signatures each including a sequence of characters;  
3 (b) combining the list of virus signatures into a tree of virus signatures including a  
4 plurality of branches each including a sequence of characters, wherein at least a  
5 portion of the branches includes upper branch portions and lower branch  
6 portions;  
7 (c) obfuscating the sequence of characters in the tree of virus signatures;

- 8 (d) comparing the data against the upper branch portions of the tree;
- 9 (e) comparing the data against the lower branch portions of the tree if the data was
- 10 successfully compared to the upper branch portions associated with the lower
- 11 branch portions;
- 12 (f) declaring a virus signature to be recognized upon the successful comparison of
- 13 the data against an entirety of at least one branch of the tree that includes all of
- 14 the characters of one of the virus signatures; and
- 15 (g) determining that the data is eligible to be declared clean upon the unsuccessful
- 16 comparison of the data against an entirety of at least one branch of the tree that
- 17 includes all of the characters of one of the virus signatures.

09916714.032601